IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Canceled).

Claim 2 (Previously Presented): The system of claim 6, wherein the communications engine uses SSL to create a secure communications link with the client.

Claim 3 (Previously Presented): The system of claim 6, wherein the communications engine negotiates an encryption protocol for transferring messages to and from the client.

Claim 4 (Previously Presented): The system of claim 6, wherein the communications engine uses public key certificates for transferring messages to and from the client.

Claim 5 (Previously Presented): The system of claim 6, wherein the security services use public key certificates to authenticate a user of the client to determine the user privileges.

Claim 6 (Currently Amended): A system on a server computer system, comprising:

a communications engine ~~for establishing~~ configured to establish a communications link with a client;

a security services engine coupled to the communications engine ~~for presenting~~ configured to present to ~~a user of~~ the client a plurality of user authentication protocol options, each user authentication protocol option having a particular level of authentication associated with it~~, for authenticating~~ to authenticate ~~the~~ a user according to at least one user authentication protocol and ~~for determining~~ to determine user privileges based on the identity of the user and the level of authentication;

a web server engine ~~for presenting~~ configured to present a set of available services based on the user privileges, at least one of the available services requiring additional authentication information to be provided before access to the service is granted~~, and for enabling~~ to enable the client to select a particular service from the set of available services;

a host engine coupled to the security services engine and to the web server ~~for providing~~ configured to provide to the client executable service communication code that enables communication with the particular service; and

a keysafe ~~for storing keys~~ configured to store keys, each key for enabling communication between the client and a ~~respective~~ service selected from the set of available services and including all additional authentication information required by the ~~respective~~ selected service for authenticating the user to the ~~respective~~ selected service, the executable service communication code functioning to retrieve a key corresponding to the particular service selected from the keysafe upon execution of the code~~ thereby enabling the client to access the available services without storing the service communication code and keys at the client or having to carry or remember them~~.

Claim 7 (Canceled).

Claim 8 (Previously Presented): The system of claim 6, wherein the security services use a digital signature to authenticate the user to determine the user privileges.

Claim 9 (Previously Presented): The system of claim 6, wherein the host engine forwards to the client security code for enabling the client to perform a security protocol recognized by the security services.

Claim 10 (Previously Presented): The system of claim 6, wherein one of the available services is secured by a firewall and one of the keys includes the additional authentication information to enable communication through the firewall.

Claim 11 (Previously Presented): The system of claim 6, further comprising a firewall for protecting the system.

Claim 12 (Previously Presented): The system of claim 6, wherein one of the keys includes an address identifying the location of the selected service.

Claim 13 (Previously Presented): The system of claim 6, wherein the code uses a key to provide to the client a direct connection with the selected service.

Claim 14 (Previously Presented): The system of claim 6, further comprising a proxy for communicating with the selected service, and wherein the code enables the client to communicate with the proxy and one of the keys enables the proxy to locate the selected service.

Claim 15 (Canceled).

Claim 16 (Previously Presented): The method of claim 20, wherein establishing a communications link includes the step of using SSL to create a secure communications link with the client.

Claim 17 (Previously Presented): The method of claim 20, wherein establishing a communications link includes the step of negotiating an encryption protocol for transferring messages to and from the client.

Claim 18 (Previously Presented): The method of claim 20, wherein establishing a communications link includes the step of using public key certificates for transferring messages to and from the client.

Claim 19 (Previously Presented): The method of claim 20, wherein determining user privileges includes the step of using public key certificates to authenticate a user of the client.

Claim 20 (Currently Amended): A ~~computer-based~~ method comprising:

establishing a communications link with a client;

presenting to ~~a user of~~ the client a plurality of user authentication protocol options, each user authentication protocol option having a particular level of authentication associated with it;

authenticating the user according to at least one user authentication protocol option;

determining user privileges based on the identity of a user and the level of authentication;

presenting a set of available services based on the user privileges, at least one of the available services requiring additional authentication information to be provided before access to the service is granted;

enabling the client to select a particular service from a set of available services;

providing to the client executable service communication code that enables communication with the particular service; and

retrieving a key from a set of keys, each key corresponding to a respective service from the set of available services, the retrieved key for enabling communication between the client and the particular service selected and including all additional authentication information required by the ~~respective~~ selected service for authenticating the user to the ~~respective~~ selected service, the executable service communication code functioning to retrieve a key corresponding to the particular service selected from the keysafe upon execution of the code ~~thereby enabling the client to access the available services without storing the service communication code and keys at the client or having to carry or remember them~~.

Claim 21 (Canceled).

Claim 22 (Previously Presented): The method of claim 20, wherein determining user privileges includes ~~the step of~~ using a digital signature to authenticate the user.

Claim 23 (Previously Presented): The method of claim 20, wherein establishing a communications link includes forwarding to the client security code for enabling the client to perform a recognized security protocol.

Claim 24 (Previously Presented): The method of claim 20, further comprising:

~~the step of~~ using one of the keys to communicate through a firewall to the selected service.

Claim 25 (Previously Presented): The method of claim 20, wherein the method is performed by a server ~~and further comprising using~~ employing a firewall to protect the server.

Claim 26 (Previously Presented): The method of claim 20, wherein one of the keys includes an address identifying the location of the selected service.

Claim 27 (Previously Presented): The method of claim 20, wherein providing includes the step of providing to the client a direct connection with the service.

Claim 28 (Previously Presented): The method of claim 20, further comprising:

using a proxy to communicate with the service, and wherein providing includes enabling the client to communicate with the proxy.

Claim 29 (Currently Amended): A system on a server computer system, comprising:

means for establishing a communications link with a client;

means for presenting ~~to a user of~~ the client a plurality of user authentication protocol options, each user authentication protocol option having a particular level of authentication;

means for authenticating ~~the~~ a user according to at least one user authentication protocol;

means for determining user privileges based on the identity of ~~a~~ the user and the level of authentication;

means for presenting a set of available services based on the user privileges, at least ~~on~~ one of the available services requiring additional authentication information to be provided before granting access to the service;

means for enabling the client to select a particular service from a set of available services;

means for providing to the client executable service communication code that enables communication with the particular service; and

means for retrieving a key from a set of keys, each key corresponding to a respective service from the set of available services, the retrieved key for enabling communication between the client and the particular service selected and including all additional authentication information required by the ~~respective~~ selected service for authenticating the user to the ~~respective~~ selected service, the executable service communication code functioning to retrieve a key corresponding to the particular service selected from the keysafe upon execution of the code~~thereby enabling the client to access the available services without storing the service communication code and keys at the client~~.

Claims 30-39 (Canceled)